VERKKOSIVUJEN TIETOTURVALLISUUDEN TESTAAMINEN JA PARANTAMINEN

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulun opinnäytetyö

HAMK, Tietojenkäsittelyn koulutusohjelma

Visamäki, syksy 2018

Mikko Lehtinen

Hämeen Ammattikorkeakoulu
Tradenomi
Tietojenkäsittely

Tekijä Mikko Lehtinen **Vuosi** 2018

Työn nimi Verkkosivujen tietoturvallisuuden testaaminen ja parantaminen

Työn ohjaaja Tommi Saksa

TIIVISTELMÄ

Opinnäytetyön aiheena oli verkkosivujen tietoturvallisuuden testaaminen ja parantaminen. Opinnäytetyössä kerrottiin lukijalle yleisimmistä kotisivuja vastaan kohdistuvista uhista, sekä siitä kuinka hyökkäykset yleensä toteutetaan ja kuinka niihin voitiin etukäteen varautua.

Opinnäytetyön ensimmäisessä käytännön osuudessa tehtiin laadullisena tutkimuksena teemahaastatteluja, joiden pohjalta tehtiin kartoitusta pienyritysten johtajien tietoturvatietämyksestä ja heidän suhtautumisestaan yrityksen kotisivuihin kohdistuviin uhkiin. Käytännön osuuden toisessa osassa tutustuttiin ja testattiin neljää eri kotisivujen tietoturvaa testaavaa ilmaispalvelua ja vertailtiin niitä keskenään palvelujen sisällön ja helppokäyttöisyyden suhteen.

Näiden tutkimusten pohjalta voitiin todeta, että haastatellut pienyritykset panostavat itse melko vähän kotisivujen tietoturvaan ja jättävät tietoturvan hoitamisen palveluntuottajalle, vaikka tietoturvan testaaminen on itsekin melko yksinkertaista ja selkeää. Valtaosa haastatelluista henkilöistä kertoi saaneensa lisää tietämystä kotisivuihin kohdistuvista uhkista viime vuosien aikana. Kuitenkaan kukaan haastatelluista ei ollut ryhtynyt mihinkään konkreettisiin toimiin riskien hallitsemiseksi tai ehkäisemiseksi.

Avainsanat Tietoturva, Verkkohyökkäykset, Tietomurto ja WWW-sivustot.

Sivut 25 s.

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Häme University of Applied Sciences
Bachelor of Business Administration

Author	Mikko Lehtinen	**Year** 2018
Subject of Bachelor's Thesis	Website security	
Supervisors	Tommi Saksa	

ABSTRACT

The subjects of this Bachelor's thesis are testing and improving the security of web pages. The Thesis describes the threats to the reader about the most common websites, how the attacks against them are carried out and how to prepare websites for future attacks.

The first practical part of the Bachelor's thesis is a qualitative study made with theme interviews. Interviews are made to survey the knowledge of web page security from small business leaders and their attitudes to threats to companies' web pages. In the second part of the practical part, four Internet services are tested that test the website security free of charge. These services are tested and their contents are compared to each other and analyzed how easy they are to use.

Based on the practical part of the thesis it can be claimed that interviewed companies put relatively little effort to the web page security and let their service provider take care of it, although it wouldn't take a lot of working hours to test it yourself. Most of the interviewees reported that they had gained more knowledge of the threats posed to the web sites. However, none of the interviewees had taken any concrete steps to control or prevent the risks.

Keywords Cyber security, Web Attacks, Data Breach and Web Sites.

Pages 25 p. + appendices XX p.

Sanasto

CMS	Content Management System, Julkaisujärjestelmä
DDoS	a Distributed Denial of Service, Palvelunestohyökkäys
SQLi	SQL Injection, SQL-injektio
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
Phishing	Verkkourkinta
XSS	Cross-Site Scipting, Tietoturva-aukko haittakoodin syöttämiseksi
MitM	Man-in-the-Middle, Epärehellinen välittäjä tai välistävetohyökkäys
Brute-force	Brute-Force on hyökkäys, joka perustuu moneen peräkkäiseen salasanan arvaus yritykseen
ERP	Enterprise Resource Planning, tuotannonohjaus järjestelmä
Bot	Laite tai ohjelma joka suorittaa toimintoja automaattisesti
TCP	Transmission Control Protocol, lähetyksen ohjausprotokolla
SSH	Secure Shell, salattuun tietoliikenteeseen tarkoitettu protokolla

SISÄLLYS

1 JOHDANTO

Monesti kotisivuja hankittaessa kiinnitetään huomiota ulkoasuun, ominaisuuksiin ja hintaan. Tietoturvasta harvoin puhutaan mainospuheissa ja se onkin asia, jonka usein vain oletetaan olevan kunnossa. Valtaosa moderneista kotisivuista tehdään valmiiden pohjien päälle jo olemassa olevista moduuleista ja toiminnallisuuksista. Tämä mahdollistaa kevyemmällä työmäärällä näyttävämpien ja muokkautuvampien kotisivujen tekemisen, mutta tuo mukanaan myös haasteita. (Ipage 2017.)

Tutkimuksessa käydään läpi, millaisia uhkia kotisivuille kohdistuu ja mitä niiden ennaltaehkäisemiseksi olisi tehtävissä. Internetin dataliikenteestä yli puolet on bottien liikennettä (Lafrance 2017). Viimeisen viiden vuoden aikana noin joka kolmas verkkosivujen kävijä oli automatisoitu hyökkäysbotti (Lafrance 2017). Pienten yritysten sivut ovatkin usein automatisoitujen hyökkäysten kohteita heikomman tietoturvan johdosta. Suurin syy heikkoon tietoturvaan on se, että yritykset uskovat olevansa liian pieniä kohteita hakkereille. Monet pienyrittäjät ovatkin kiireisiä, eivätkä he ole edes miettineet tietoturva-asioita. Vaikka he yleisesti ovat tietoisiamonenlaisista tietoturvariskeistä, niiden usein ei uskota koskettavan omaa liiketoimintaa. (Ipage 2017.)

Tutkimusongelmaksi työssä nouseekin tietoturvakysymykset pienyrittäjien näkökulmasta. Tuleeko yrittäjien kiinnitettyä tietoturvaan tarvittavaa huomiota, kun kaikki muutkin yrityksen hoitoon liittyvät asiat tulisi hoitaa?

Tutkimuskysymykset ovat seuraavat:

Minkälaisia hyökkäyksiä pk-yritysten kotisivuille voi kohdistua ja mitä haittaa niistä voi seurata?
Kuinka tärkeäksi pk-yrityksissä koetaan tietoturva- asiat?
Voiko yrittäjä testata itse kotisivujensa turvallisuutta ja kuinka tämä tehdään?

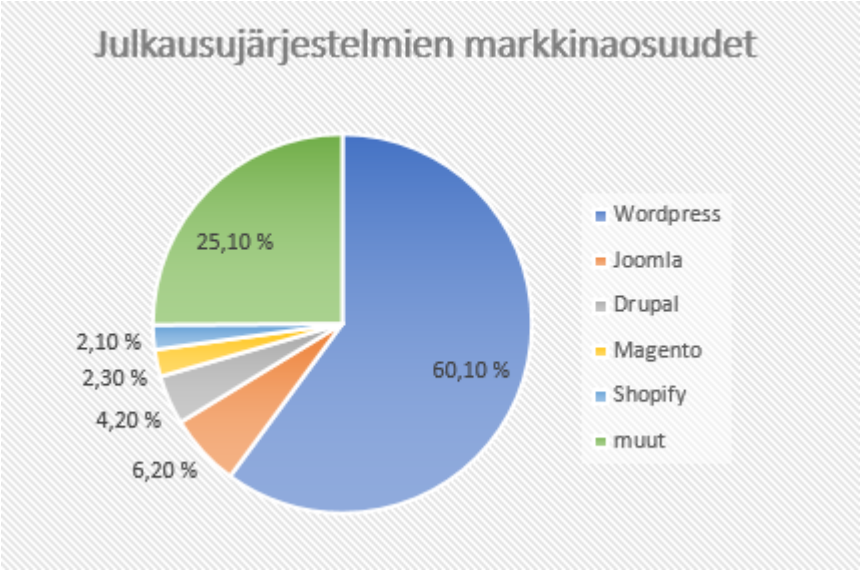
Tässä opinnäytetyössä tehty tutkimus on haastattelun ja havainnoinnin keinoin toteutettu laadullinen tutkimus. Lisäksi toisena tutkimusmetodina on käytetty käytännön testausta. Haastattelun pienen otannan vuoksi tutkimustuloksia ei voida yleistää suurempaan mittakaavaan, mutta auttaa osiltaan vastaamaan tutkimusongelmaan ja sen mukanaan tuomiin kysymyksiin. Tutkimuksen tavoitteena on luoda kuvaa, kuinka tärkeäksi pk-yrityksissä tietoturva koetaan ja kuinka paljon siitä tiedetään, tai ymmärretään. Lisäksi tavoitteena on ymmärtää pienyritysten kotisivujen tietoturvaa ja siihen liittyvien käsitteiden, riskien ja ilmiöiden luonnetta. Työssäni it-alalla törmään säännöllisesti tietoturvakysymyksiin ja tämän kautta olen ollut kiinnostunut syventymään aiheeseen enemmän.

2 KOTISIVUJEN TIETOTURVA

Kotisivut ovat yrityksen julkinen näyteikkuna. Se on usein asiakkaan ensikosketus yritykseen ja luo ensivaikutelman yrityksestä. Jos kotisivut eivät ole tietoturvalliset, kriittisiä asiakastietoja voi vuotaa yrityksen ulkopuolelle. Jos sivusto on saastunut viruksesta. se voi kerätä sellaisia asiakastietoja, kuten nimi, sähköpostiosoite, sosiaaliturvatunnus, tai luottokortin numero ja maksutiedot, tai käyttää sivustoa hyväksi hyökkäyksissä. Saastunut sivusto voi lähettää roskapostia ja viruksia asiakkaalle yrityksen nimissä. Jo yksikin tietoturvavuoto voi pilata yrityksen maineen ja pahimmillaan ajaa yrityksen konkurssiin mahdollisilla sakoilla ja korvauksilla, jotka tietomurto voi tuoda mukanaan (Ipage 2017).

Nykyään yhä useammalla kotisivulla on linkityksiä kotisivujen sisäverkossa toimiviin palveluihin, kuten intranettiin tai tuotannonohjausjärjestelmään, johon voidaan tehdä kyselyitä kotisivujen kautta. Tällaisessa tapauksessa kotisivujen laiminlyöty tietoturva saattaa toimia takaporttina hyökkääjälle, jota kautta avautuu pääsy suojattuun sisäverkkoon. Uusia hyökkäyksiä ja haavoittuvuuksia löydetään jatkuvasti ja niihin tehdään paikkauksia ja korjauksia moduulien ja ohjelmien tekijöiden toimesta (Lafrance 2017). Valtaosa automatisoiduista hyökkäyksistä olisikin estettävissä ajallaan tehtyjen päivitysten avulla (Ipage 2017).

Julkaisujärjestelmällä tarkoitetaan toiminnallisuutta, jolla helpotetaan kotisivujen sisällönhallintaa siten, että teksti ja kuvat voidaan lisätä hallinta työkalusta eikä koodaustaitoa tarvita. Useimmat nykyaikaiset kotisivut toteutetaankin julkaisujärjestelmää hyväksikäyttäen sisällön päivittämisen helppoudesta johtuen. Moni julkaisujärjestelmä perustuu avoimeen lähdekoodiin ja yleisimpiä esimerkkejä näistä ovat WordPress, Joomla, Drupal ja Magento. WordPress on näistä suosituin ja se pyörittää noin 29% kaikista internetin sivustoista (Karol 2018).



Kuva 1. Julkaisujärjestelmien markkinaosuudet.

Pelkästään WordPress julkaisujärjestelmästä on löydetty 3972 haavoittuvuutta, joista 52% lisäosissa, 37% WordPressissä itsessään ja 11% WrodPressin teemoissa (wpscan 2017). Oikein käytettynä ja turvallisuus ohjeita ja käytäntöjä noudatettuna WordPress kuten muutkin julkaisujärjestelmät ovat todella tietoturvallinen. (Kristen 2017.)

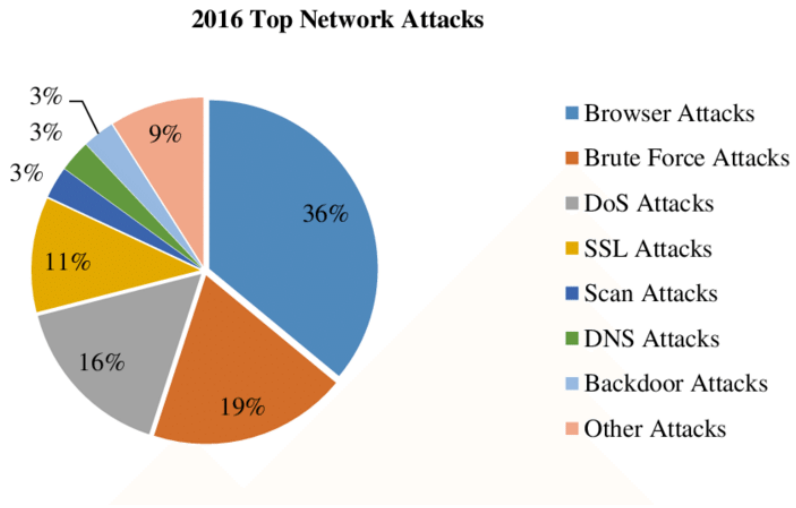
Kotisivuja tehdessä usein käyttöön valikoituu viimeisimmät versiot julkaisujärjestelmistä ja muista kotisivuille tulevista lisätoiminnoista, mutta ilman ylläpitosopimusta niiden päivittäminen useimmiten unohtuu ja jää jopa kokonaan tekemättä. Tämä johtaa siihen, että kotisivujen tietoturva heikkenee ajan myötä, kun uusia haavoittuvuuksia löydetään ja paikkauksia niihin ei ole asennettuna. (Kristen 2017.) Wordpressin tietojen mukaan vain noin 22% sitä käyttävistä sivustoista on uusin versio päivitettynä, ja noin 18% sivustoista ei ole vielä päivitetty vuonna 2014 julkaistuun versioon 4.0 tai sen yli (Karol 2018).

3 TIETOTURVAHYÖKKÄYKSET

Tietoturvahyökkäykset voidaan ryhmitellä karkeasti kahteen eri ryhmään; automatisoidut ja kohdennetut hyökkäykset.

Automatisoiduissa hyökkäyksissä hyökkääjän käskyttämä botti etsii satunnaisia sivustoja internetistä ja kokeilee nopeasti, löytyykö kyseisestä sivustosta etsittyjä haavoittuvuuksia. Haavoittuvuutta vastaan hyökätään joko heti, tai sivusto lisätään toisen botin listalle, joka tekee hyökkäyksen. Automatisoidussa hyökkäyksessä yleisimmin laitetaan hyökkääjän mainoksia etusivulle, tai kaapataan sivuston sähköpostipalvelu, joka valjastetaan lähettämään roskapostia ja mainoksia. Tietoturvayhtiö Impervan tekemässä tutkimuksessa analysoitiin yli 16,7 miljardia kävijää 100 000 satunnaisesti valikoidulla sivustolla jotka ovat heidän verkossa. Tarkastetuista sivustoista 94,2% oli kohdistunut automatisoituja hyökkäysyrityksiä 90 päivän tarkastelujakson aikana. Valtaosa näistä hyökkäyksistä käyttävät hyväkseen jo yleisesti tunnettuja haavoittuvuuksia, tai toiminta malleja. (Perez 2016).

Kohdennetuissa hyökkäyksissä kohteeksi valikoituu sellainen taho, jolle halutaan tehdä vahinkoa, tai jolta voidaan kiristää, tai varastaa arvokasta tietoa. Usein nämä kohteet ovat isoja kansainvälisiä sivustoja, joiden tietoturva on paremmalla tasolla, kuin monella pienemmällä yrityksellä. Tällaisia sivustoja vastaan automatisoidut hyökkäykset useimmiten eivät toimi, vaan hyökkääjät usein käyttävät viikkoja aikaa mahdollisten haavoittuvuuksien etsimiseen. (Trenndmicro 2015.)



Kuva 2. hyökkäystyyppien jakauma 2016 (ResearchGate 2016).

3.1 SQL-injektio (**SQLi**)

SQL-injektiolla tarkoitetaan hyökkäystä, jossa kotisivulla olevaan täydennettävään kenttään syötetään haittakoodia. Kaikkia SQL-injektiohyökkäyksiä yhdistää se, että syötettävä haittakoodi on SQL-tietokanta kyselyn koodia. (Netsparker n.d.) SQL-injektioon ei ole olemassa täysin varmuudella toimivaa suojaa, mutta on olemassa monia keinoja, joiden avulla turvallisuutta voidaan parantaa. Näistä yleisimpiä ovat kenttään syötettävän datan rajoittaminen, jolloin estetään merkit, joita haettavassa datassa ei voi olla. Esimerkiksi kentässä, jossa haetaan henkilöä nimellä, voidaan estää numerot ja erikoismerkit. Ohjelmallisesti suojausta voidaan parantaa käyttämällä verkkosovellus palomuuria, joka monitoroi dataliikennettä. Tämä tunnistaa ja estää haittakoodin syöttöyrityksiä. Yleisesti hyvä käytäntö on käyttöoikeuksien rajaaminen tietokannassa siten, että SQL-kyselyt käyttävät sellaisia tunnuksia, joilla on oikeudet vain niiden tarvitsemaan dataan. Tämä ei estä tietomurtoa, mutta rajoittaa sen laajuutta. Säännölliset tietoturvapäivitykset ovat tehokas suojaus automatisoituja hyökkäyksiä vastaan. Kun kaupallisista palveluista löytyy tietoturva-aukkoja, ne pyritään paikkaamaan mahdollisimman nopeasti. (Weiss 2016.)

Jos SQL-injektioon ei ole varauduttu ollenkaan, hyökkääjä voi tehdä tietokannassa hakuja, lisäyksiä, poistoja ja muokkauksia dataan, ladata itselleen arkaluonteista tietoa tai tyhjentää koko tietokannan (Weiss A). Esimerkkitilanne, jossa sivuston käyttäjä syöttää $user ja $password muuttujien tiedot sivuilta, SQL-kysely näyttää tältä:

```
$statement = "SELECT * FROM users WHERE username = '$user' AND password = '$password'";
```

Hyökkääjä syöttää yksinkertaisen koodin kenttään ja suoritettava kysely näyttää tältä:

```
$statement = "SELECT * FROM users WHERE username = 'admin' ; --'AND password = '$password'";
```

Tässä vihreä teksti on hyökkääjän syöttämä koodi ja harmaa teksti on kommentoitua koodia. Tämä tapahtuu sen takia, että kyselyssä on puolipiste, joka SQL-kielessä tarkoittaa lausekkeen lopetusta. Tämän jälkeen tulee kaksi viivaa, jotka tarkoittavat, että loppurivi on kommenttia, eikä suoritettavaa koodia. Tämä koodi poistaa salasanan tarkastuksen kokonaan ja kirjaa käyttäjän sisään järjestelmänvalvojatunnuksilla ilman salasanaa. (Netsparker.n.d)

Sony Networksin palveluihin murtauduttiin yksinkertaisella SQL-injektio menetelmällä. Suojaukset olivat puutteellisia ja hyökkäys toteutettiin nopealla aikataululla. Vain kolmessa päivässä sivustolle saatiin täydet admin oikeudet ja sieltä ladattiin mm. 75 000 musiikkikoodia, 3,5 miljoonaa musiikkikuponkia ja yli miljoonan käyttäjän käyttäjätunnus ja salasana suojaamattomana (Vijayan 2011). Murron tutkinnassa vahvistettiin, että hakkerien käyttämät menetelmät olivat yksinkertaisia ja opittavissa muutamassa tun-

nissa internetissä olevista tutoriaalivideoista (Martin 2011). Hyökkäys aiheutti merkittäviä taloudellisia ja imagollisia vahinkoja Sonylle (Vijayan 2011).

3.2 Palvelunestohyökkäys (**DDoS**)

Palvelunestohyökkäyksellä tarkoitetaan hyökkäystä, jolla kuormitetaan sivustoa tai palvelua niin paljon, että sen kapasiteetti loppuu ja se lakkaa vastaamasta käyttäjilleen. Hyökkäyksen vaikutus voi vaihdella pienestä hidastumisesta aina kokonaisten sivustojen kaatumiseen (Hulme 2018). Palvelunestohyökkäysten tehosta kertoo paljon se, että monella valtiolla on oma virtuaalisen sodankäynnin osasto, ja esimerkiksi Ukrainan sodassa sitä käytetiin aktiivisesti hyväksi tietokatkosten luomiseksi (Deane-McKenna 2016). Hyökkäykset perustuvat internetin protokollien heikkouksiin. Kun protokollia on aikoinaan suunniteltu, ei ole otettu huomioon, että niitä voi käyttää myös väärin. Uusissa hyökkäyksissä usein hyödynnetään vanhoja toiminnallisuuksia, vuonna 1983 verkkotulostinten testaustarpeisiin julkaistu CHARGEN-protokolla on hyvä esimerkki tästä. Protokolla itsessään on harmiton mutta se palauttaa 200-1000 kertaisen määrän tietoa lähetettyyn verrattuna. jolloin se kuormittaa kohdetta merkittävästi hyökkääjää enemmän. (Saarenlainen 2016).

Palvelunestohyökkäyksiä on tehty pitkään, mutta 2000-luvun alussa ne tuli suuren yleisön tietotisuuteen kanadalaisen Michael Calcen toimesta joka oli hyökkäyksiä tehdessään 15-vuotias. Hän valjasti yliopistojen tietokoneverkot tekemään samanaikaisia yhteydenottopyyntöjä kohdesivustolle ja kaatoi ne täysin. Viikon sisällä hän onnistui saamaan 6 isoa sivustoa polvilleen, mukaan lukien Aim, Amazon, CNN, eBay ja Yahoo. (Hersher 2015.)

DDoS-hyökkäys vaatii taakseen bottiverkoston. Useimmiten se koostuu saastutetuista laitteista, joilla on pääsy internetiin. Laitteeksi kelpaa niin reitittimet, tulostimet, puhelimet, kuin älytelevisiotkin. (Incapsula2 n.d.) Palvelunestohyökkäysiin ei ole olemassa täydellistä suojaa, joka estäisi hyökkäykset kokonaan, mutta on olemassa keinoja, joilla hyökkäykseen voidaan varautua. On olemassa fyysisiä laitteita, jotka kykenevät analysoimaan yhteyksiä ja estämään haitallisia yhteydenottopyyntöjä, mutta niilläkin on rajallinen kapasiteetti ja ison hyökkäyksen edessä ne ovat voimattomia. Yleisin suojautumiskeino on käyttää pilvipalveluita, jossa iso palveluntarjoaja omaa paljon kapasiteettia ja edistyneet laitteistot, joiden kapasiteetti riittää isompaankin hyökkäykseen. Pilvipalveluissa liikennettä voidaan ohjata helposti uudelleen toisille palvelimille, jotka eivät ole hyökkäyksen kohteena ja näin ollen ylläpitää palvelun toiminta. (Saarelainen 2016.)

Hyökkäyksiä on neljää eri päätyyppiä:

TCP-hyökkäys	Otetaan niin monta yhteyttä, että laitteisto ei pysty hallitsemaan niitä jolloin aiheutuu laitteiston kaatuminen.
Volyymihyökkäys,	Käytetään verkon kaikki datansiirto kapasiteetti, jolloin yhteys hidastuu tai katkeaa kokonaan.
Fragmentaatio-hyökkäys	Lähetetään massoittain puutteellisia TCP kutsuja jolloin kohde yrittää korjata niitä ja kapasiteetti loppuu.
Ohjelmakohtainen-hyökkäys	Hyödynnetään ohjelmien raskaita toimintoja, jolloin hyökkääjien määrä on pienempi tehden siitä vaikeammin havaittavan ja estettävän hyökkäyksen.

Taulukko 1. (Digitalattackmap 2013).

3.3 Väsytyshyökkäys (**Brute-force**)

Brute-force -hyökkäyksessä, eli väsytyshyökkäyksessä hyökkääjä käyttää joukkoa ennalta määritettyjä arvoja, lähettää käskyn kohteeseen ja analysoi vastaustauksia onnistumiseen asti. Hyökkäyksen onnistuminen riippuu määritellyistä arvoista. Mitä suurempi otanta on kyseessä, sitä enemmän se vie aikaa, mutta onnistuu paremmalla todennäköisyydellä. Yleisin ja helpoin ymmärrettävä esimerkki Brute-force -hyökkäyksestä on sanakirjahyökkäys salasanan murtamiseksi. Tässä hyökkääjä käyttää salasanakirjastoa, joka sisältää miljoonia sanoja, joita voidaan käyttää salasanana. Hyökkääjä yrittää näitä mahdollisia salasanoja yksitellen ja jos tämä sanakirja sisältää oikean salasanan, hyökkäys onnistuu.

Perinteisessä Brute-force -hyökkäyksessä hyökkääjä yrittää kirjaimia ja numeroita yhdistelemällä luoda oikeaa salasanaa. Tämä perinteinen tekniikka kestää kauemmin, kun salasana on riittävän pitkä. Nämä hyökkäykset voivat kestää useita minuutteja useita tunteja tai useita vuosia riippuen käytetystä järjestelmästä ja salasanan pituudesta.

Käänteinen Brute-force -hyökkäys on menetelmä, joka liittyy salasanan hakkerointiin. Tässä hyökkääjä yrittää arvata salasanan useilta käyttäjätunnuksilta. Tätä käytetään silloin, kun tiedetään salasana, mutta ei käyttäjätunnusta.

Brute-force -hyökkäyksessä voidaan käyttää myös muilta verkkosivustoilta vuodettuja käyttäjätunnus- ja salasanapareja ja yrittää päästä samoilla kirjautumistiedoilla johonkin toiseen verkkopalveluun.

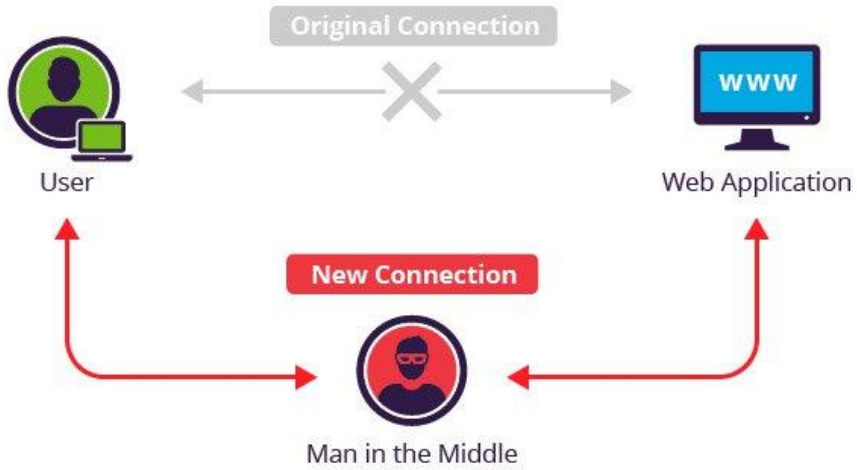
Brute-force menetelmää voidaan käyttää myös piilotettujen sivujen löytämiseksi. Hyökkääjä yrittää keksiä piilotetun sivun nimen ja lähettää sille kutsun ja analysoi vastauksen. (Shankdhar 2015.) Väsytyshyökkäyksiä vas-

taan ei ole täysin varmaa suojaa, mutta hyökkäyksen onnistumisen todennäköisyyttä voidaan pienentää merkittävästi. Yleisimmin käytettyihin suojauksiin kuuluvat tarpeeksi pitkä ja monimutkainen salasanavaatimus, käyttäjätunnuksen lukkiutuminen toistuvien epäonnistuneiden kirjautumisyritysten jälkeen, CAPTCHA:n lisääminen sivulle, joka vaikeuttaa ja voi jopa pysäyttää hyökkäyksen ja käyttäjien valveutuneisuus vahvan salasanan valinnassa. (Owasp 2016.) Vahva salasana on vaikea murtaa, jos se ei pidä sisällään sanakirjan sanoja, nimiä, peräkkäisiä numeroyhdistelmiä, ei ole käytössä muilla sivustoilla ja se vaihdetaan useasti. (Owasp 2016.)

Loka-marraskuun vaihteessa 2015 Alibaba verkkosivustoon kohdistui massiivinen Brute-force -hyökkäys. Hyökkäyksessä käytettiin hyväksi tietokantaa, joka koostui 99 miljoonasta käyttäjätunnus-salasana-yhdistelmästä, jotka oli vuotaneet muilta verkkosivuilta. Hakkerit pääsivät käsiksi lähes 21 miljoonalle käyttäjätilille. Joka viides näistä yrityksistä oli onnistunut mikä viittaa siihen, että käyttäjillä on usein samat käyttäjätunnukset ja salasanat useilla eri sivustoilla (Buntinx 2017.)

3.4 Välistävetohyökkäys (**MitM**)

MitM-hyökkäyksestä käytetään melko kuvaavia suomenkielisiä termejä; välistävetohyökkäys, epärehellinen välittäjä ja mies välissä. Hyökkäys toteutetaan niin, että hyökkääjä ohjaa kulkevan liikenteen oman laitteensa kautta ja esittäytyy verkkopalvelulle hyökkäyksen kohteena ja hyökkäyksen kohteelle verkkopalveluna (Kuva1). MitM-hyökkäyksessä voidaan seurata ja muuttaa lähetettäviä ja vastaanotettavia tietoja. Hyökkäykset yleisesti toteutetaan avoimissa WLAN-verkoissa, joita nykyisin on lähes kaikkialla tarjolla. Hyökkäykset usein kohdistetaan sivustoihin ja henkilöihin, joilta voi saada arvokasta tietoa, kuten pankkien, tai isojen yritysten kirjautumistietoja.



Kuva 3. Välistävetohyökkäys (incapsula n.d.).

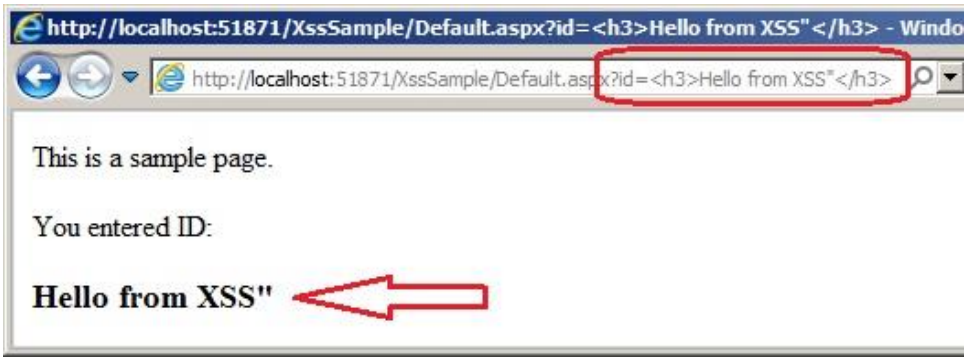
Välistävetohyökkäykseen voidaan varautua verkkosivujen ylläpitäjän toimesta käyttämällä salattua HTTPS-yhteyttä ja sertifikaatteja (Owasp 2016).

Tämän lisäksi on mahdollista seurata palvelimen ja käyttäjän välillä tapahtuvien pyyntöjen viivettä, jolloin poikkeuksellinen viiveen pidentyminen viittaisi mahdolliseen välistävetohyökkäykseen (Aziz & Hamilton 2009, 81-86).

Suurempi vaikutus suojautumiseen on sivustojen käyttäjällä. Avoimia langattomia verkkoja tulisi välttää, selaimen varoituksiin sivuston turvallisuudesta tulee kiinnittää huomiota sekä muistaa kirjautua suojatuista palveluista ulos, kun niitä ei enää käytä. (Owasp 2016).

3.5 Koodinsyöttöhyökkäys (**XSS**)

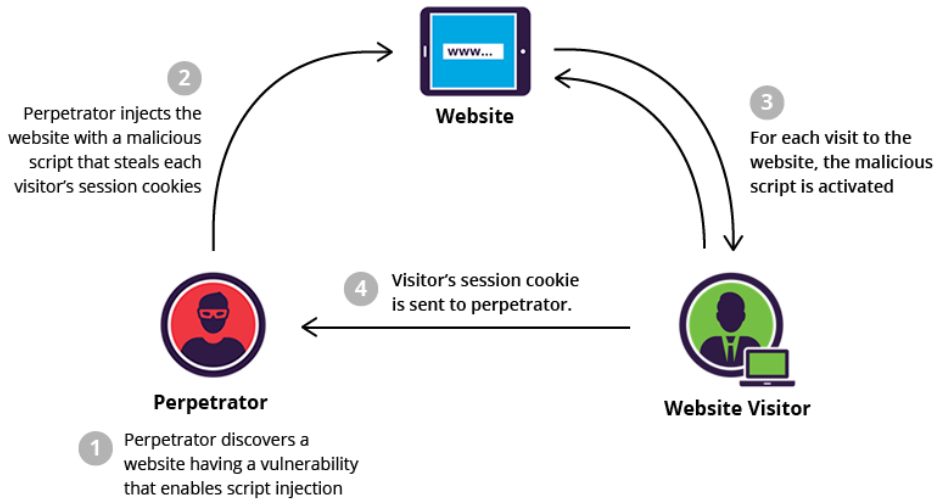
Koodinsyöttöhyökkäyksessä hyväksikäytetään tunnettuja tietoturva-aukkoja, jotka mahdollistavat kotisivuille ulkopuolisen koodin syöttämisen. Tietoturva-aukon hyödyntäminen mahdollistaa pääsynhallinnan kiertämisen. Käytännössä joko sivustolle itsessään syötetään haittakoodia, tai sitä lisätään sivuston linkin sisälle, mikä saa verkkosivuston käyttäytymään halutulla tavalla. (Herbrandson 2014.)



Kuva 4. Linkkiin lisätty haittakoodi (Singh 2013).

Tiettyyn henkilöön kohdistetuissa hyökkäyksissä hyökkäys tapahtuu välillisesti haavoittuvuuden sisältävien sivustojen kautta, joissa kohde vierailee. Sivustoa käytetään haitallisen koodin välittämiseksi kohteen selaimelle. Koodinsyöttöhyökkäyksessä hyödynnetään jonkin verran VBScriptiä, ActiveX ja Flashia, mutta yleisimmin se kohdistuu JavaSciptiin, koska sitä käytetään lähes kaikilla kotisivuilla. (Acunetix n.a..)

Valtaosa koodinsyöttöhyökkäyksistä kuitenkin toteutetaan ilman, että se kohdistuu tiettyyn henkilön. Tällöin kohteita ovat kaikki kyseistä sivustoa käyttävät henkilöt. Esimerkki tapauksessa hyökkääjä saastuttaa haavoittuvan sivuston koodillaan, joka kerää sivustolla vierailevien henkilöiden tunnistautumisevästeet ja lähettää ne hyökkääjälle (Kuva4). Kun hyökkääjä vierailee sivustolla kyseisillä evästeillä, sivusto tunnistaa evästeen ja päästää hyökkääjän kohteen tunnuksilla sisälle palveluun. (CodePlex n.d.)



Kuva 5. Koodinsyöttöhyökkäys (incapsula n.d.).

Koodinsyöttöhyökkäykseen ennaltaehkäisemiseksi yleisimmät keinot ovat epäluotettavan tiedon rajoittaminen, merkkien siistiminen ja suojaus kirjastot. Epäluotettava tieto tarkoitetaan tietoa, joka tulee ulkoisesta lähteestä kuten sivulla olevasta kentästä. Tällaista tietoa saa suoraan syöttää html script tagiin, kommenttiin, attribuutin nimeen, tagin nimeen tai CSS-tyyliin. Koodin siistimisessä merkit, joita käytetään tagin vaihtamiseksi, muutetaan heksa muotoon. Tällöin merkki tulostuu samannäköisenä käyttäjälle, mutta sitä ei voida käyttää koodin suorittamiseen. Tällaisia merkkejä ovat & < > ” ’ ja /. Nämä merkit voidaan muuttaa muotoon & < > " ' ja &#xF; (owasp2 2018). Suojauskirjastot ovat valmiita koodipaketteja, johon on kasattu toimintoja, jotka ovat tarkoitettu estämään koodinsyöttöhyökkäyksiä. Vaihtoehtoja tähän löytyy useita, kuten Microsoftin Web Protection Library, jonka yhtenä osana on AntiXSS-kirjasto (CodePlex n.d.).

Historiassa yksi tunnetuimmista tapauksista on Myspace-palvelussa ollut tietoturva-aukko. Käytännössä käyttäjä lisäsi omaan profiiliinsa koodin, joka automaattisesti kopioi koodin katsojan profiiliin ja lisäksi lähetti hakkerille kaveripyynnön. Tämä mahdollisti koodin eksponentiaalisen leviämisen, ja jo vuorokauden kuluessa koodi oli saastuttanut yli miljoona profiilia. MySpace-joutui sulkemaan sivustonsa selvittääkseen mistä tässä oli kyse. Kyseinen hyökkäys oli laajasti uutisoitu tapahtuessaan vuonna 2006 ja se on edelleen kaikkien aikojen nopeimmin levinnyt virus. (Franceschi-Bicchierai 2015.)

4 AINEISTON KERÄÄMINEN JA ANALYYSI

Tämä opinnäytetyö toteutettiin laadullisena tutkimuksena. Laadullisin menetelmin tehty tutkimus tarkastelee ihmisten ja merkitysten maailmaa ja sen avulla pyritään ymmärtämään sellaisia syyseuraussuhteita, joita ei muilla tutkimusmenetelmillä kyettäisi havainnoimaan. Menetelmällä tutkitaan ihmisten merkitykselliseksi kokemia tapahtumaketjuja, jotka liittyvät monisyisesti arvoihin ja valintoihin. (Vilkka 2005, 97; Hirsjärvi, Remes & Sajavaara 2004, 155.) Työn aineistonkeruu- ja analysointimenetelmiä ovat teemahaastattelu, sisällön analyysi ja toissijaisena tutkimusmuotona käytännön testaus, joka toteutettiin anonyymin kotisivun tietoturvallisuuden testauksena. Käytännön testaus ei ole perinteinen menetelmä kvalitatiivisessa tutkimuksessa, mutta työn ja tutkimuksen luonteen huomioiden se tuo työhön arvokasta lisätietoa, sekä laajentaa yleisesti ymmärrystä aihealueesta. Laadullisessa tutkimuksessa aineisto on tarkoitus kerätä tavoilla, jotka vievät tutkijan tutkittavan kohteen lähelle. Yleisimpiä tapoja ovat tässäkin työssä käytettävät haastattelu ja havainnointi. Aineistolähtöisesti tehtävässä aineiston analyysissa jäsennetään aineiston kautta merkitykselliseksi tulkitut teemat. Koska aineistoa pyritään ymmärtämään suhteessa kontekstiin, viitekehykseen ja aihealueen erityispiirteisiin, on sitä tutkittava kokonaisvaltaisesti ja moniulotteisesti. (Kiviniemi 2001, 68–69.)

4.1 Teemahaastattelu

Haastatteluja on monenlaisia, kuten täysin avoimia, puolistrukturoituja, tai täysin strukturoituja. Haastattelut voi toteuttaa kasvotusten, puhelimitse, kahden kesken, ryhmässä, tai lomakehaastatteluna. Puolistrukturoitua haastattelua nimitetään myös teemahaastatteluksi. Teemahaastattelu tuo yleensä esiin asioita, joita ei tiedosteta jokapäiväisessä elämässä, kuten arvoja, perusteluja ja toimintaa ohjaavia uskomuksia. (Metsämuuronen 2011, 114-115.) Tässä opinnäytetyössä teemahaastattelu tuo esiin arvoja liittyen tietoisuuteen tietoturva-asioista, arvoihin toiminnan takana ja auttaa täten ymmärtämään syitä tietoturvan silloiseen tilaan.

4.2 Sisällön analyysi

Sisällönanalyysi on tekstianalyysia ja sen avulla kuvataan aineiston inhimillistä sisältöä. (Tuomi, Sarajärvi 2002, 93.) Aineistolähtöinen sisällönanalyysi koostuu eri työvaiheista. Aineiston pelkistäminen on ensimmäinen työvaihe. Pelkistäessä aineistosta karsitaan tutkimustehtävän kannalta epäolennainen tieto. Sen jälkeen aineisto täytyy ryhmitellä ja lopuksi luoda teoreettiset käsitteet. Aineiston tiivistäminen ja pilkkominen ovat tapoja pelkistää aineistoa. Pelkistämisen jälkeen on määritettävä analyysiyksikkö, jotta aineistoa voidaan alkaa analysoimaan. Analyysiyksikkönä voi toimia esimerkiksi yksittäinen sana, tai laajempi lausekokonaisuus. (Tuomi & Sarajärvi 2002, 110–113.)

Tätä aineistoa analysoidessa analyysiyksikkönä toimi tietyt teemasanat. Haastatteluista poimittiin ne teemasanat ja teemat, jotka liittyivät kotisivujen rakenteeseen, päivityksiin, tietoturvaan ja hyökkäysten ehkäisemiseen.

5 HAASTATTELUTUTKIMUKSEN TULOKSET

Haastatteluissa otanta on työtuntien rajallisuuden vuoksi hyvin pieni. Tästä syystä tutkimustulos on enemmänkin suuntaa antava, kuin varsinaisesti yleistyskelpoinen.

Haastatteluja tehtiin yhteensä kahdeksan. Näistä seitsemän on yrityksiä, joilla on kotisivut käytössä ja yksi on yritys, joka tekee ja ylläpitää kotisivuja suomalaisille asiakkaille.

5.1 Haastateltavien esittely

Haastatelluista kotisivujen omistajista löytyy eri alojen yrityksiä, kuten verkkokauppoja, sosiaalialan yritys, ja pienlaitehuoltoytitys. Yritykset työllistävät 3-8 henkeä ja ovat perustettu 2-24 vuotta sitten.

IT-talo Devnet Oy on perustettu vuonna 2005 ja työllistää noin 25 henkeä. Toiminta jakautuu kolmeen pääalueeseen: koodaus, konesali palvelut ja IT-palveluiden ulkoistus. Toimitusjohtaja Peter Thim arvioi, että kotisivuja on tehty tänä aikana arviolta 500 kappaletta ja verkkokauppoja on kymmeniä. Kaikille tehtäville sivuille tulee julkaisujärjestelmä, useimmiten käytetään omaa julkaisujärjestelmää tai Wordpressiä. Verkkokauppa alustana käytetään avoimen lähdekoodin verkkokauppa ratkaisua nimeltä Prestashop.

Kotisivuja myydään ylläpitosopimuksella ja ilman. Valtaosa nykyisin myytävistä kotisivuista myydään ylläpitosopimuksella. Asiakkaiden tietoisuus tietoturva uhkia kohtaan on selkeästi kasvanut ja ylläpitosopimuksen hyödyt tiedostetaan helpommin.

5.2 Kotisivujen rakenne

Haastatteluissa ilmeni, että kaikilla otannan kotisivuilla oli käytössä julkaisujärjestelmä. Kaksi haastatelluista tunnisti oman sivustonsa julkaisujärjestelmän Joomlaksi mutta lopuilta viideltä asiasta ei löytynyt tietoa. Kaksi sivustoa sisälsi verkkokaupan. Molemmat verkkokaupat oli ostettu palveluna palveluntarjoajalta. Vain yksi kotisivuista oli ilman ylläpito sopimusta, loput kuusi oli ylläpitosopimuksellisia. Sopimusten sisällöstä ei ollut tarkempaa tietoa mutta yleinen käsitys oli, että toimittaja hoitaa tietoturva päivitysten tekemisen ja kuluttaja sisällön tuottamisen.

5.3 Kotisivujen sisältö

Haastateltujen yrittäjien kotisivuista millään ei itsessään ollut tallessa arkaluonteiseksi luokiteltavaa tietoa, kuten henkilötietoja, tai maksukorttien tietoja. Verkkokaupoilla on asiakasrekisterit mutta palvelun tarjoaja ylläpitää niitä toisella palvelimella. Kotisivujen, joilla ei ollut verkkokauppoja päätarkoitus oli oleellisen informaation tuottaminen asiakkaille.

5.4 Tietoisuus hyökkäysyrityksistä ja niistä raportointi

Haastatelluista kolme kertoi saavansa säännöllisesti raportteja tietoturvapäivityksistä, hyökkäyksistä ja uusista toiminnallisuuksista mitä julkaisujärjestelmään tai verkkokauppaan on tullut. Neljä kertoi, ettei mitään ilmoituksia ole tullut ja haastatellut olivatkin epävarmoja siitä, että onko ylläpitäjällä edes mitään seurantaa olemassa.
Kahdelle sivustoista oli kohdistunut tietoturvahyökkäyksiä, toiselle sivustolle oli tehty koodinsyöttö hyökkäys ja toisen sähköpostilaatikko oli kaapattu lähettämään roskapostia.

> Ei ole tullut mitään ilmoituksia. Sähköposti oli joskus kaapattu ja siitäkään ei tullut mitään ilmoitusta. Kun asiasta ylläpitäjälle raportoin, sitä ei otettu alkuun edes tosissaan vaan sanottiin roskapostien liittyvän johonkin muuhun asiaan.
>
> Kotisivun omistaja 1

> Devnetin ylläpidossa on tuhansia kotisivuja ja murtautumisia ja murtautumisyrityksiä tulee viikoittain. pääsääntöisesti hyökkäykset tapahtuvat julkaisujärjestelmän vanhempaa versiota hyödyntäen tai julkaisujärjestelmässä käytettäviä kolmannen osapuolen moduulien heikkouksista, joita pyritään välttämään. jonka takia sivujen rakentamisessa onkin tärkeä tietää, miten se tehdään oikein, jotta siellä on huomioitu tietoturva. omasta suljetusta julkaisujärjestelmästä ei ole ikinä päästy läpi, koska se on tuntematon hyökkääjille ja siihen tulee paljon vähemmän kohdistettuja hyökkäyksiä.
>
> Peter Thim

5.5 Tietoturvatietoisuus

Kaikki haastatellut olivat omien sanojensa mukaan tulleet tietoisemmiksi mahdollisista uhista ja hyökkäyksistä viimeisen kahden vuoden aikana. Ymmärrys siitä, että hyökkäyksiä ei tehdä vain isoja yrityksiä vastaan on lisääntynyt ja osalle haastatelluista hyökkäyksiä on myös konkreettisesti kohdalle osunut. Tarkempaa teknistä ymmärrystä asiasta haastatelluilla kotisivujen omistajilla ei ollut ja tietoturvan testaaminen ja parantaminen jääkin kotisivujen toimittajan vastuulle.

> ”Nyt näiden kysymysten jälkeen huoli tietoturvasta on kasvanut, varsinkin kun aiempi sähköpostin kaappaus on osunut omalle kohdalle”
>
> Kotisivun omistaja 1

6 KOTISIVUJEN TIETOTURVALLISUUDEN TODENTAMINEN

Kotisivujen tietoturvallisuuden todentaminen voidaan joko tehdä itse, tai ostaa palveluna. Jos kotisivut on ostettu palveluna, tietoturva yleisesti ottaen kuuluu palvelun tarjoajalle. Testaus olisi hyvä tehdä säännöllisin aikavälein, koska uusia haavoittuvuuksia ja hyökkäyksiä löytyy jatkuvasti. Uusia haavoittuvuuksia sivustolle saattaa tulla myös päivitysten ja uusien toiminnallisuuksia mukana. Isompien muutosten jälkeen kotisivulle olisikin hyvä tehdä tietoturvatarkastus. (Ipage 2017.) Kotisivujen tietoturvan testaamiseksi on olemassa lukuisia eri vaihtoehtoja. Vaihteluväli on valmiiksi tuotetusta palvelusta aina tietoturvatestaukseen erikoistuneeseen Linux julkaisuun asti, jossa kaikki testaus tehdään itse käsin. Testattavaksi kotisivuksi valikoitui käytössä oleva palvelu, jonka oletettiin sisältävän joitain haavoittuvuuksia.

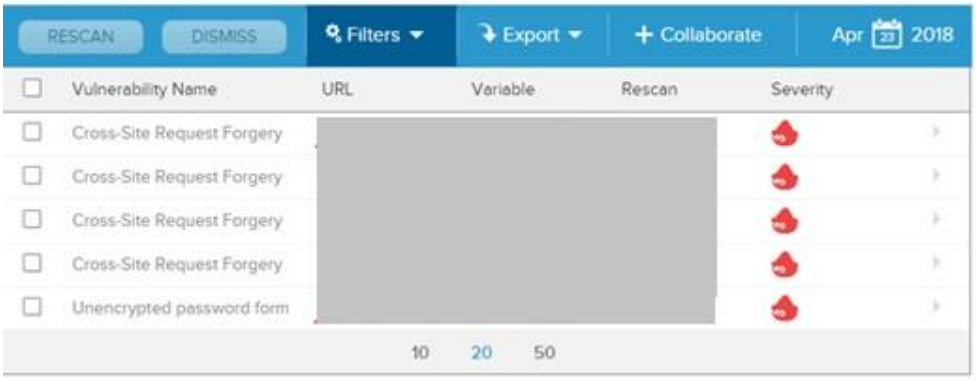
Testisivusto haluttiin pitää anonyyminä sivuston ja sen käyttäjien suojelemiseksi. Sivustolle voidaan kirjautua sisään ja sinne ladataan kuvia ja tekstiä. Sivustolla ei kerätä tai säilötä arkaluontoista henkilökohtaista dataa eikä sillä ole käytössä verkkomaksuja. Testisivustoa tyypillisesti käytetään puhelimilla paikoissa jossa yleisiä langattomia verkkoja ei ole saatavilla, joten käyttö pääpainoisesti tapahtuu omalla mobiilidatalla. Testaamiseen valikoitui **SaaS** (Software as a Service) mallin mukaisia palveluna tuotettuja testejä. Kaikilla palveluilla tehdyt testit olivat ilmaisia tehdä, osa koeajan ja osa jatkuvasti.

6.1 Tinfoil Security

Ensimmäiseksi testisivustoksi valikoitui Tinfoil Security, palvelussa on ilmainen kuukauden koeaika, jonka jälkeen palvelu muuttuu maksulliseksi. Tunnusten luominen, sähköpostin varmentaminen ja sivuston varmentaminen piti tehdä, jotta palvelun sai käyttöön. Sivuston autentikointiin käytetiin etusivulle lisättävää metadataa.

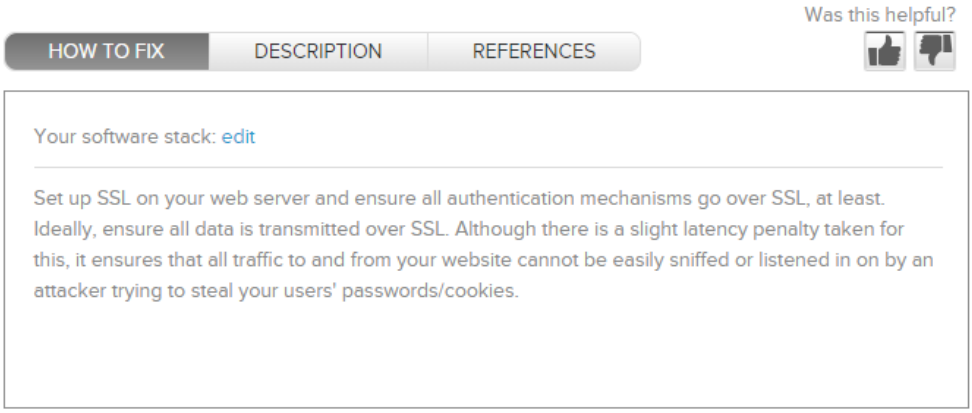
Kuva 6. Sivuston autentikointi metadatalla.

Kun sivusto oli autentikoitu, tietoturvatestauksen pystyi aloittamaan. Palvelun ajaminen kesti noin 45 minuuttia, jonka jälkeen sivustolle aukesi raportti löydetyistä haavoittuvuuksista. Haavoittuvuuksien riskit oli arvioitu asteikolla korkea, keskitaso, matala ja informatiivinen. Haavoittuvuuksia löytyi yhteensä 16 kappaletta, joista viisi olivat korkean riskin haavoittuvuuksia. Näistä neljä liittyi koodinsyöttöhyökkäykseen ja yksi suojaamattomaan salasanakäsittelyyn.



Kuva 7. Tinfoil Security korkean riskin haavoittuvuudet.

Raportti on selkeästi muotoiltu, vain oleellinen tieto on aluksi näkyvillä ja sitä saa helposti lisää näkyviin. Raportti antaa korjausehdotukset jokaisesta haavoittuvuudesta ja tarkemman kuvauksen siitä, miten sitä voitaisiin hyväksikäyttää mahdollisessa hyökkäyksessä.



Kuva 8. Tinfoil Security salasanan käsittelyn korjausehdotus.

6.2 Scan My Server

Scan My Server-palvelusta valittiin ilmainen ”Basic” palveluntaso, jolla tietoturvatestaukset ajettiin. Rekisteröinti vei noin kaksi minuuttia, mutta testin ajaminen vaati linkin lisäämisen etusivulle, jossa näkyy palveluntarjoajan logo ja tietoa viimeisimmästä testistä.

Kuva 9. Scan My Server palvelun sivulle lisättävä tunniste.

Tunnustenluonnin yhteydessä sivusto luo html koodipätkän, jonka lisäämällä etusivulle logon saa näkyviin ja testauksen käynnistettyä. Testaus suoritetaan vuorokauden kuluessa sen käynnistämisestä ja siitä tulee ilmoitus sähköpostiin, kun se on suoritettu.

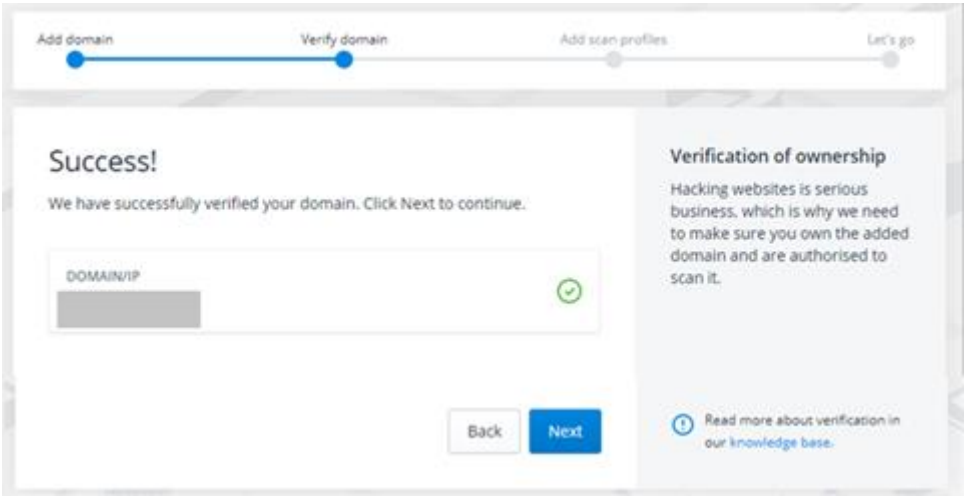
Scan My Server-palvelun raportissa haavoittuvuudet oli luokiteltu kolmeen eri riskiluokkaan: korkea, keskitaso ja matala. Testejä tehtiin yhteensä 16034 kappaletta, joissa löytyi 15 haavoittuvuutta. Näistä viisi oli luokiteltu keskitasoisiksi ja 10 matalaksi. Keskitason haavoittuvuuksista yksi liittyi 64 bittisessä SSL-salauksessa olevaan haavoittuvuuteen, joka tunnetaan nimellä Sweet32 Birthday. Hyökkäyksessä hyödynnetään 64 bittisen salauksen purkuavain määrää. Tämä raja saadaan ylittymään, jos dataa siirretään 32 GB jonka jälkeen kaikki tarvittavat salausavaimet ovat hyökkääjän tiedossa. Loput neljä liittyivät evästeiden suojaamiseen, jossa evästeitä välitetään salaamattomina jolloin epärehellinen välittäjä saattaa päästä näihin käsiksi. Raportin rakenne on selkeä ja haavoittuvuuksien linkeistä pääsee helposti käsiksi tarkempiin tietoihin ja korjausehdotuksiin.

Scan Results	
Hostname	[redacted]
Scan date	2018-04-23
Scan Status	Done
Vulnerability Score	59.05 (F)
Vulnerability Summary	
High	0
Medium	5 Sweet32 Birthday Attacks on 64-bit Block Ciphers in TLS and OpenVPN (DES-CBC3) Web Application Cookies Lack Secure Flag Web Application Cookies Lack Secure Flag Web Application Cookies Lack HttpOnly Flag Web Application Cookies Lack HttpOnly Flag
Low	10 SSH Server Backported Security Patches HTTP Packet Inspection HTTP Packet Inspection Supported SSL Ciphers Suites Identify Unknown Services via GET Requests Identify Unknown Services via GET Requests Identify Unknown Services via GET Requests SSL Verification Test NTP Variables Reading ICMP Timestamp Request
Total	15

Kuva 10. Scan My Server palvelun raportti.

6.3 Detectify

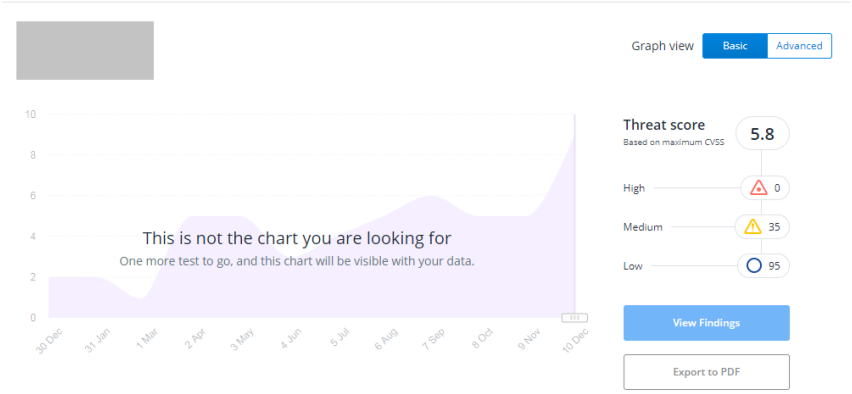
Detectify-palvelu on kuukausimaksullinen ja sitä saa kokeilla ilmaiseksi 14 päivää. Palvelun käyttäminen vaatii rekisteröinnin, sähköpostin vahvistamisen ja sivuston autentikoinnin, joka tapahtuu lataamalla sivustolle palveluntarjoajan antama tiedosto. Rekisteröinti ja sivuston autentikointivalikot ovat selkeitä ja yksiselitteisiä.



Kuva 11. Detectify sivuston rekisteröinti.

Noin viidessä minuutissa rekisteröinti on tehty ja pääsee valitsemaan palvelun tason. Testiin valittiin ilmainen koeaika, jolla palvelu käynnistettiin. Tarkastus kesti noin 45 minuuttia jonka jälkeen sähköpostiin tuli ilmoitus, että testaus on suoritettu ja raportti on luettavissa palveluntarjoajan sivulla. Haavoittuvuudet arvioitiin asteikolla korkea, keskitaso ja matala ja niitä löytyi yhteensä 130, joista 35 oli keskitason luokituksella ja 95 matalan tason luokituksella. Raportin erittelyssä keskitason haavoittuvuuksissa oli

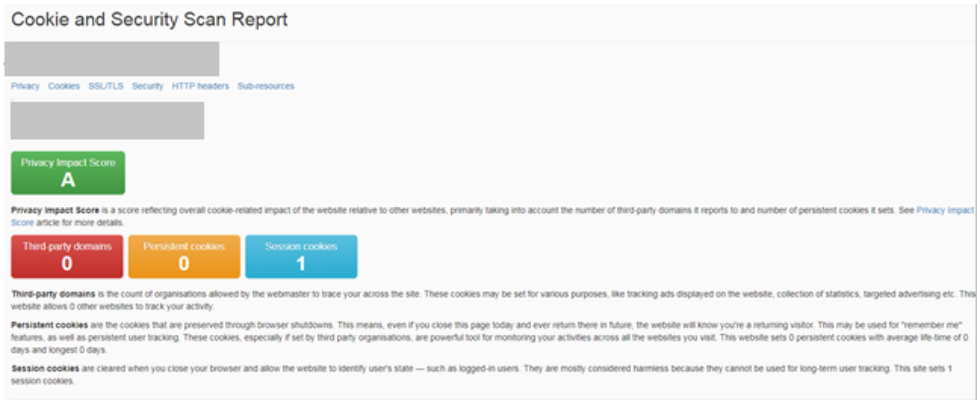
huomattavissa kaksi selkeää trendiä. Haavoittuvuuksista 13 liittyi koodinsyöttö hyökkäyksiin ja 14 liittyi sivuston rakenteen ja polkujen suojaamiseen. Raportissa pääsee tarkastelemaan tarkemmin, mistä haavoittuvuus löytyi ja tarkempaa selitystä, miten hyökkääjät voivat hyväksikäyttää sitä. Raportissa on korjausehdotukset ja selitykset niiden vaikutuksista käyttäjille.



Kuva 12. Detectify sivuston raportti.

6.4 Web Cookies Scanner

Web Cookies Scanner tarkastelee sivustolla käytettyjä evästeitä. Testi on täysin ilmainen. Se ei vaadi rekisteröintiä, tai sivuston ylläpito-oikeuksien tarkastamista, vaan kuka tahansa voi ajaa testin mille tahansa sivustolle. Sivuston testaaminen kestää noin 30 sekuntia ja raportti tulee suoraan selaimeen näkyviin. Raportissa eritellään ulkopuolisten sivustojen evästeet, pysyvät evästeet ja istuntokohtaiset evästeet. Testisivusto sai yksityisyydensuojasta parhaan arvosanan, koska sivustolla ei ole kolmannen osapuolen evästeitä, eikä pysyviä evästeitä. Istuntokohtaisia evästeitä on yksi, joka on välttämätön kirjautumistietojen säilyttämistä varten. Raportissa itsessään on selitetty selkeästi mihin eri evästeitä käytetään ja kuinka se vaikuttaa sivuston käyttäjän yksityisyyteen.



Kuva 13. Web Cookie Scanner raportti.

6.5 Yhteenveto testeistä

Käytetyistä palveluista Scan My Server, Tinfoil Security ja Detectify testasivat kotisivuilla olevia tietoturvahaavoittuvuuksia, kun taas Web Cookie Scanner tarkasteli sivustoa käyttäjän yksityisyyden näkökannalta. Kuten aiemmin nähdyistä raporteista voi päätellä, yksikään testeistä ei ollut täysin samanlainen. Haavoittuvuuksia löytyi eri määriä ja niiden luokittelussa oli eroja, mutta yhtenäisyyksiäkin niistä löytyi. Yhtäkään SQL-injektioon liittyvää haavoittuvuutta ei löydetty ja kaikilla raporteilla oli huomautettavaa evästeiden suojaamisesta ja heikosta SSH-suojauksesta. Scan My Server ei löytänyt koodinsyöttö haavoittuvuuksia, mutta Tinfoil securityn ja Detectifyn -palvelussa ne nousivat selkeästi esille. Tästä voikin päätellä, että eri palveluntarjoajien testeissä on selkeitä eroja. Täytyy toki huomioida, että ilmaisversioiden testit ovat suppeammat, kuin maksullisissa palveluissa, joka voi osaltaan selittää raporttien välisiä eroja. Joka tapauksessa raportit antavat hyvän yleiskatsauksen sivuston yleisestä turvallisuudesta.

Kaikista raporteista koostetussa yhteenvedossa arvioisin sivuston riittävän turvalliseksi sen käyttötarkoitukseen. Koodinsyöttöhyökkäyksen toteuttaminen kyseiselle sivustolle on epätodennäköistä, ja istuntoevästeiden kaappaamisella ei voi saada suurta vahinkoa aikaan. Pienillä muutoksilla yli puolet haavoittuvuuksista saataisiin paikattua. Näistä tärkeimpinä pitäisin SSH-protokollan tiukentamista siten, että helposti murrettavissa oleva 3DES-salausprotokolla vaihdettaisiin turvallisempaan AES-protokollaan. Toinen tärkeä muutos olisi evästeiden suojaamista. Nykyisellään istunto evästeet käyttävät suojaamatonta http-yhteyttä suojatun HTTPS-protokollan sijaan. Tämän lisäksi evästeille olisi hyvä lisätä ’secure’ atribuutti, joka parantaa niiden suojausta. Sivuston polut ja rakenne eivät ole suojattuja, vaan ne ovat katsottavissa sivustolta. Suojaamattomuus ei itsessään ole haavoittuvuus, mutta hyökkääjä voi hyödyntää näitä tietoja hyökkäystä tehdessään.

7 YHTEENVETO

Tutkimuksessa tultiin siihen lopputulokseen, että ajantasaisilla tietoturvapäivityksillä ja pienellä perehtymisellä kotisivujen tietoturva saadaan pidettyä hyvällä tasolla. Uusia haavoittuvuuksia löydetään jatkuvasti ja niihin tehdään paikkauksia. Suurimmat riskit yleensä kohdistuvat vanhoihin versioihin kotisivujen lisäosista ja ohjelmista, joita ei ole asianmukaisesti päivitetty.

Haastattelujen aikana yksi yleisimmäksi noussut kommentti oli se, että haastateltu kertoi tulleensa paljon tietoisemmaksi kotisivuihin kohdistuvista riskeistä. Tämän huomioiden olikin hieman yllättävää huomata, ettei kukaan kuitenkaan ollut tehnyt mitään konkreettista kotisivujen tietoturvan parantamiseksi. Tästä tulin siihen johtopäätökseen, että vaikka riskeistä ollaan melko tietoisia, ei niiden ehkä kuitenkaan uskota realisoituvan omalla kohdalla.

Tutkimusta tehdessä itselle isoimpana yllätyksenä tuli automatisoitujen hyökkäysten määrän suuri kasvu suhteessa ihmisten tekemiin hyökkäyksiin. Tämä varmaankin osaltaan selittää sen, miksi haastatellut henkilöt olivat tulleet tietoisemmiksi riskeistä.

Mielestäni tutkimus vastasi melko hyvin tutkimuskysymyksiin, haastattelujen otanta olisi voinut olla hieman suurempi ja olisin toivonut, että olisin saanut pari kotisivuja tekevää yritystä haastateltua enemmän. Valitettavasti haastattelujen saaminen kyseisen alan yrityksiltä osoittautui haastavaksi.

LÄHTEET

Acunetix. (2018.). Cross-site Scripting (XSS) Attack. https://www.acunetix.com/websitesecurity/cross-site-scripting/ Viitattu 12.4.2018

Aziz, B. & Hamilton G. (2009.). Detecting Man-in-the-Middle Attacks by Precise Timing.
1. painos. Ateena: IEEE. Viitattu 12.4.2018

Buntin, J. (2017.). *The Merkle.* Top 5 Brute Force Attacks. Viitattu 21.3.2018
https://themerkle.com/top-5-brute-force-attacks/

CodePlex. (n.d.) CodePlex Archives. viitattu 26.4.2018
https://archive.codeplex.com/?p=wpl

Digitalattackmap. (2013.). What is a DDoS Attack?. Viitattu 20.3.2018
https://www.digitalattackmap.com/understanding-ddos/

Deane-McKenna, C. (2016.). The next Cold War has already begun – in cyberspace. Viitattu 20.3.2018
http://theconversation.com/the-next-cold-war-has-already-begun-in-cyberspace-57367

Franceschi-Bicchierai L. (2015.). *Motherboard* The MySpace Worm that Changed the Internet Forever. https://motherboard.vice.com/en_us/article/wnjwb4/the-myspace-worm-that-changed-the-internet-forever Viitattu 12.4.2018

Hersher, R. (2015.). Meet Mafiaboy, The 'Bratty Kid' Who Took Down The Internet Viitattu 20.3.2018
https://www.npr.org/sections/alltechconsidered/2015/02/07/384567322/meet-mafiaboy-the-bratty-kid-who-took-down-the-internet

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2004.). *Tutki ja kirjoita.* 10. osin uud. p. Helsinki: Kustannusosakeyhtiö Tammi.

Hulme, G. (2018.). How distributed denial of service attacks are evolving.
Viitattu 20.3.2018
https://www.csoonline.com/article/3222095/network-security/ddos-explained-how-denial-of-service-attacks-are-evolving.html

Ipage. (2017.). *Why Web Security is Important*. Viitattu 22.3.2018
http://ipage.com/blog/why-web-security-is-important/

Incapsula. (n.d.). Man In The Middle (MITM) Attack. Viitattu 12.4.2018
https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html

Incapsula2. (n.d.). Botnet DDoS attacks. https://www.incapsula.com/ddos/botnet-ddos.html
viitattu 4.5.2018

Karol K. (2018.). WordPress Stats: Your Ultimate List of WordPress Statistics https://www.codeinwp.com/blog/wordpress-statistics/ Viitattu 18.4.2018

Kiviniemi, K. (2001.). *Laadullinen tutkimus prosessina.* Teoksessa Aaltola, J., Valli, R. (toim.) 2001. Ikkunoita tutkimusmetodeihin 2. Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. Jyväskylä: Gummerus Kirjapaino Oy, 68–69.

Kuva2 (n.d.). Viitattu 4.5.2018 https://www.researchgate.net/figure/Top-seven-network-attack-types-in-2016_fig6_321637905

Kuva3. (n.d.). Incapsula Viitattu 12.4.2018 https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html

kuva3. Singh, R. (n.d.). Codeproject An Absolute Beginner's Tutorial on Cross Site Scripting(XSS) Prevention in ASP.NET https://www.codeproject.com/Articles/573458/An-Absolute-Beginners-Tutorial-on-Cross-Site-Scrip Viitattu 25.4.2018

Kuva4. Incapsula. (n.d.). Viitattu 12.4.2018 https://www.incapsula.com/web-application-security/cross-site-scripting-xss-attacks.html

Kristen W. (2017.). 5 Common WordPress Security Issues https://ithemes.com/2017/01/16/wordpress-security-issues/ Viitattu 18.4.2018

Lafrance, A. (2017.). *The Internet Is Mostly Bots*. Viitattu 18.3.2018 https://www.theatlantic.com/technology/archive/2017/01/bots-bots-bots/515043/

Metsämuuronen, J. (2006.). *Laadullisen tutkimuksen käsikirja*. Jyväskylä: Gummerus Oy.

Martin, A. (2011.). LulzSec's Sony Hack Really Was as Simple as It Claimed. Viitattu 20.3.2018 https://www.theatlantic.com/technology/archive/2011/09/lulzsecs-sony-hack-really-was-simple-it-claimed/335527/

Netsparker. (n.d.). What is the SQL Injection Vulnerability. Viitattu 20.3.2018 https://www.netsparker.com/blog/web-security/sql-injection-vulnerability/

Owasp2. (2018.). XSS (Cross Site Scripting) Prevention Cheat Sheet https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet Viitattu 26.4.2018

Owasp. (2016.). Brute force attack. Viitattu 21.3.2018 https://www.owasp.org/index.php/Brute_force_attack

Perez, R. (2016.). SC Magazine Imperva: in 2016, 94.2% of websites experienced a bot attack
https://www.scmagazineuk.com/imperva-in-2016-942-of-websites-experienced-a-bot-attack/article/634233/
Viitattu 9.5.2018

Saarelainen, A. (2016,). Tietoviikko. Dos-hyökkäys kaataa nettipalvelun. Viitattu 20.3.2018
https://www.tivi.fi/Kaikki_uutiset/dos-hyokkays-kaataa-nettipalvelun-miten-voi-suojatua-6535679

Shankdhar, P. (2015.). Popular Tools for Brute-force Attacks. Viitattu 21.3.2018
http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref

TrendMicro. (2015.). What is a Targeted Attack?
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-what-is-a-targeted-attack
viitattu 4.5.2018

Tuomi, J & Sarajärvi, A. (2003.). *Laadullinen tutkimus ja sisällönanalyysi.* Jyväskylä: Gummerus Oy.

Vijayan, J. (2011.). Sony Pictures falls victim to major data breach.
Viitattu 20.3.2018
https://www.computerworld.com/article/2508871/network-security/sony-pictures-falls-victim-to-major-data-breach.html

Vilkka, H. (2005.). Tutki ja kehitä. Helsinki: Otavan kirjapaino.

Weiss A. (2016.). How to Prevent SQL Injection Attacks. Viitattu 20.3.2018
https://www.esecurityplanet.com/hackers/how-to-prevent-sql-injection-attacks.html

WPScan. (n.d.) https://wpscan.org/
Viitattu 18.4.2018